09/890280 PCT/JP00/00475

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

28.01.00
REC'D 17 MAR 2000
WIPO PCT

EJU

#3

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年 １月２９日

出願番号
Application Number: 平成１１年特許願第０２１２５４号

出願人
Applicant (s): 株式会社日立製作所

２０００年 ３月 ３日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号 出証特２０００－３０１１５７２

【書類名】　特許願

【整理番号】　K99000151

【提出日】　平成11年 1月29日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

【発明の名称】　公開鍵暗号方法

【請求項の数】　14

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　西岡　玄次

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100068504

【弁理士】

【氏名又は名称】　小川　勝男

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　公開鍵暗号方法

【特許請求の範囲】

【請求項１】

送信者は，受信者の公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって，

（１）鍵情報生成のステップとして，

【数１】

$$\bullet\ p,\ q\text{:prime numbers}$$
$$\bullet\ s \in \mathbf{Z}\ (gh^s \equiv 1 \pmod{p}) \qquad \cdots(数1)$$

なる前記秘密鍵（p,q,s）を作成し，さらに，

【数２】

$$\bullet\ g,\ h,\ k \in \mathbf{Z}\ (0 < g, h < n)$$
$$\bullet\ n = p^d q \quad (d \geq 1) \qquad \cdots(数2)$$

なる前記公開鍵（n,g,h,k）を作成し（但し，kはp,qのビット長），

（２）前記送信者は，前記公開鍵（n,g,h,k）を用いて，乱数r（$0<r<2^{k-1}$）を選び，前記送信データm（$0<m<2^{k-1}$）について，

【数３】

$$C = mg^r \bmod n,$$
$$D = h^r \bmod n \qquad \cdots(数3)$$

を計算し，C,Dを前記受信者に送信し，

（３）前記受信者は，前記秘密鍵（p,q,s）を用いて，

【数４】

$$m = CD^s \bmod p, \qquad \cdots(数4)$$

により，前記送信データmを求める

ことを特徴とする公開鍵暗号方法。

【請求項２】

送信者と受信者とが、暗号通信を行なうための鍵を共有する鍵共有方法であって，

（１）鍵情報生成のステップとして，

【数５】

- p, q:prime numbers
- $s \in \mathbf{Z}\ (gh^s \equiv 1 \pmod{p})$

・・・(数5)

なる秘密鍵（p,q,s）を作成し，さらに，

【数６】

- $g,\ h,\ k \in \mathbf{Z}\ (0 < g,h < n)$
- $n = p^d q \quad (d \geq 1)$
- f : one-way function

・・・(数6)

なる公開鍵（n,g,h,k,f）を作成し（但し，kはp,qのビット長），

（２）送信者は，前記公開鍵（n,g,h,k,f）を用いて，乱数r（$0<r<2^{k-1}$）を選び，送信データm（$0<m<2^{k-1}$）について，

【数７】

$$C = mg^r \bmod n,$$
$$D = h^r \bmod n$$

・・・(数7)

を計算し，共有鍵KをK=f(m)により計算し，前記計算結果C,Dを前記受信者に送信し，

（３）前記受信者は，前記秘密鍵（p,q,s）を用いて，

【数８】

$$m = CD^s \bmod p,$$

・・・(数8)

により，前記送信データmを求め，前記公開情報fを用いて前記共有鍵KをK=f(m)により計算する

ことを特徴とする鍵共有方法。

【請求項３】

請求項１または請求項２における前記鍵情報の作成方法であって，

受信者は，有限群G= {x∈Z/(n)|xは可逆元}の大きな位数Ｌを持つ元ξを選ぶステップを備え（但し，Z/(n)はnを法とする剰余環，Ｌはξの位数の倍数でもよい），整数α，βに対して，

【数９】

$$g = \xi^{\alpha} \bmod n, \qquad h = \xi^{\beta} \bmod n \qquad \cdots (数9)$$

とするステップを備え，さらに，

【数１０】

$$\alpha + s\beta \equiv 0 \pmod{L} \qquad \cdots (数10)$$

となるように前記秘密情報ｓを決めるステップを備える

ことを特徴とする鍵情報の作成方法。

【請求項４】

送信者は，受信者の公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって，

（１）受信者は，前記秘密鍵として，

【数１１】

- p, q:prime numbers
- $s \in \mathbf{Z}\ (gh^{s} \equiv 1 \pmod{n})$

$\cdots (数11)$

前記公開鍵として，

【数１２】

- g, h, $k \in \mathbf{Z}\ (0 < g, h < n)$
- $n = pq$

$\cdots (数12)$

を作成するステップを備え，

（２）送信者は，乱数r（0<r<k）を選び，送信データmを，

【数１３】

$$C = mg^r \bmod n,$$
$$D = h^r \bmod n \qquad \cdots(数13)$$

により，暗号化するステップを備え，

さらに，前記送信者は暗号文Ｃ，Ｄを受信者に送信するステップを備え，

（３）受信者は，

【数１４】

$$m = CD^s \bmod n, \qquad \cdots(数14)$$

により，前記送信データmを復号化するステップを備える

ことを特徴とする公開鍵暗号方法。

【請求項５】

請求項４における鍵情報の作成方法であって，

受信者は，有限群G= {x∈Z/(n)|xは可逆元} の大きな位数Ｌを持つ元ξを選ぶステップを備え（但し，Z/(n)はnを法とする剰余環，Ｌはξの位数の倍数でもよい），整数α，βに対して，

【数１５】

$$g = \xi^{\alpha} \bmod n, \qquad h = \xi^{\beta} \bmod n \qquad \cdots(数15)$$

とするステップを備え，さらに，

【数１６】

$$\alpha + s\beta \equiv 0 \pmod{L} \qquad \cdots(数16)$$

となるようにｓを決めるステップを備える

ことを特徴とする鍵情報の作成方法。

【請求項６】

請求項４における前記受信者が該送信データｍを復号化するデータ復号化方法

であって，

受信者は，

【数１７】

$$m_1 = CD^s \bmod p, \quad m_2 = CD^s \bmod q \qquad \cdots(数17)$$

を計算するステップを備え，さらに，

【数１８】

$$a \equiv 1 \pmod p, \quad a \equiv 0 \pmod q$$
$$b \equiv 0 \pmod p, \quad b \equiv 1 \pmod q \qquad \cdots(数18)$$

なる整数ａ，ｂに対して，

【数１９】

$$m = am_1 + bm_2 \bmod n \qquad \cdots(数19)$$

にて，前記送信データｍを復号化するステップを備える

ことを特徴とするデータ復号化方法。

【請求項７】

送信者は，受信者の公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって，

（１）鍵情報生成のステップとして，

【数２０】

- p, q:prime numbers
- $s_0, s_1 \in \mathbf{Z}$

$\cdots(数20)$

なる前記秘密鍵（p,q,s0,s1）を作成し，さらに，

【数２１】

- $g, h, k \in \mathbf{Z}\ (0 < g, h < n)$
- $n = p^d q\ (d \geq 1)$

$\cdots(数21)$

なる前記公開鍵（n,g,h,k）を作成し（但し，kはp,qのビット長であり，

【数２２】

$$s_i\alpha_i + \beta \equiv 0 \pmod{L} \quad (0 \leq i \leq 1) \qquad \cdots(数22)$$

とする。），

（２）前記送信者は，前記公開鍵（n,g,h,k）を用いて，乱数r（$0<r<2^{k-1}$）を選び，前記送信データm（$0<m<2^{k-1}$）についてm=m0+m1となるようにランダムにm0,m1を選ぶステップを備え，さらに，

【数２３】

$$\begin{aligned} C_0 &= m_0 g^{\alpha_0 r} \bmod n, \\ C_1 &= m_1 g^{\alpha_1 r} \bmod n, \\ D &= g^{\beta r} \bmod n, \end{aligned} \qquad \cdots(数23)$$

を計算し，(C0,C1,D)を前記受信者に送信し，

（３）前記受信者は，前記秘密鍵（p,q,s0,s1）を用いて，

【数２４】

$$m = C_0 D^{s_0} + C_1 D^{s_1} \bmod p \qquad \cdots(数24)$$

により，前記送信データmを求める

ことを特徴とする公開鍵暗号方法。

【請求項８】

請求項７において，

前記送信者は，前記送信データm（0<m<n）に対して，前記暗号化方法にて暗号文(C0,C1,D)を作成し，当該暗号文(C0,C1,D)を受信者に送信し，

前記受信者は，

【数２５】

$$m = C_0 D^{s_0} + C_1 D^{s_1} \bmod n \qquad \cdots(数25)$$

にて復号化を行う

ことを特徴とする公開鍵暗号化方法。

【請求項９】

送信者と受信者とが，暗号通信を行なうための鍵を共有する鍵共有方法であって，

（１）鍵情報生成のステップとして，

【数２６】

- p, q:prime numbers
- $s_0, s_1 \in \mathbf{Z}$

・・・(数26)

なる秘密鍵（p,q,s0,s1）を作成し，さらに，

【数２７】

- $g, h, k \in \mathbf{Z}\ (0 < g, h < n)$
- $n = p^d q\ (d \geq 1)$
- f : one-way function

・・・(数27)

なる公開鍵（n,g,h,k,f）を作成し（但し，kはp,qのビット長であり，

【数２８】

$$s_i \alpha_i + \beta \equiv 0 \pmod{L} \quad (0 \leq i \leq 1)$$

・・・(数28)

とする。），

（２）送信者は，前記公開鍵（n,g,h,k,f）を用いて，乱数r（$0<r<2^{k-1}$）を選び，送信データm（$0<m<2^{k-1}$）についてm=m0+m1となるようにランダムにm0,m1を選ぶステップを備え，さらに，

【数２９】

$$C_0 = m_0 g^{\alpha_0 r} \bmod n,$$
$$C_1 = m_1 g^{\alpha_1 r} \bmod n, \qquad \cdots(数29)$$
$$D = g^{\beta r} \bmod n,$$

を計算し，共有鍵KをK=f(m)により計算し，前記計算結果(C0,C1,D)を前記受信者に送信し，

（３）前記受信者は，前記秘密鍵（p,q,s0,s1）を用いて，

【数３０】

$$m = C_0 D^{s_0} + C_1 D^{s_1} \bmod p \qquad \cdots(数30)$$

により，前記送信データmを求め，前記公開情報ｆを用いて前記共有鍵KをK=f(m)により計算する

ことを特徴とする鍵共有方法。

【請求項１０】

送信者は，受信者の公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって，

（１）鍵情報生成のステップとして，

【数３１】

- $s \in \mathbf{Z}, \quad gh^s = 1 \ (\in H)$ $\cdots(数31)$
- H: subgroup of G

なる前記秘密鍵（s,H）を作成し，さらに，

【数３２】

- $g, h \in G$ $\cdots(数32)$
- G : finite group

なる前記公開鍵（g,h,G）を作成し，

（２）前記送信者は，前記公開鍵（g,h,G）を用いて，乱数rを選び，前記送信データm（m∈H）について，暗号文C,Dを

【数３３】

$$C = m^t g^r \ (\in G), \qquad \cdots(数33)$$
$$D = h^r \ (\in G)$$

にて計算し，該暗号文C,Dを前記受信者に送信し，

（３）前記受信者は，前記秘密鍵（s,H）を用いて，

【数３４】

$$m^t = CD^s \ (\in H), \qquad \cdots(数34)$$

を計算し，これより前記送信データmを求める

ことを特徴とする公開鍵暗号方法。

【請求項１１】

送信者と受信者とが，暗号通信を行なうための鍵を共有する鍵共有方法であって，

（１）鍵情報生成のステップとして，

【数３５】

- $s \in \mathbf{Z}, \quad gh^s = 1 \ (\in H)$
- H : subgroup of G $\qquad \cdots(数35)$

なる秘密鍵（s,H）を作成し，さらに，

【数３６】

- $g, h \in G$
- G : finite group $\qquad \cdots(数36)$
- f : one-way function

なる公開鍵（g,h,G）を作成し，

（２）送信者は，前記公開鍵（g,h,G）を用いて，乱数rを選び，前記送信データ

m（m∈H）について，暗号文C,Dを

【数３７】

$$C = m^t g^r \ (\in G), \qquad \cdots (数37)$$
$$D = h^r \ (\in G)$$

にて計算し，共有鍵KをK=f(m)により計算し，該暗号文C,Dを前記受信者に送信し，

（３）前記受信者は，前記秘密鍵（s,H）を用いて，

【数３８】

$$m^t = CD^s \ (\in H), \qquad \cdots (数38)$$

を計算し，前記送信データmを求め，公開情報ｆを用いて共有鍵KをK=f(m)により計算する

ことを特徴とする鍵共有方法。

【請求項１２】

送信者は，受信者の公開鍵を用いて送信データを暗号化し、受信者は、前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって，

（１）鍵情報生成のステップとして，

【数３９】

- p, q:prime numbers
- $s \in \mathbf{Z}$ $(gh^s \equiv 1 \pmod{pq})$

$\cdots (数39)$

なる前記秘密鍵（p,q,s）を作成し，さらに，

【数４０】

- $g, h, k \in \mathbf{Z}$ $(0 < g, h < n)$
- $n = p^d q$ $(d \geq 1)$

$\cdots (数40)$

なる前記公開鍵（n,g,h,k）を作成し（但し，kはp,qのビット長），

（２）前記送信者は，前記公開鍵（n,g,h,k）を用いて，乱数r（$0<r<2^{k-1}$）を選び，前記送信データm（$0<m<2^{k-1}$）について，暗号文C,Dを

【数４１】

$$C = m^2 g^r \bmod n, \quad \cdots (数41)$$
$$D = h^r \bmod n$$

にて計算し，該暗号文C,Dを前記受信者に送信し，

（３）前記受信者は，前記秘密鍵（p,q,s）を用いて，

【数４２】

$$m^2 = CD^s \bmod pq, \quad \cdots (数42)$$

を計算し，前記送信データmを求める

ことを特徴とする公開鍵暗号方法。

【請求項１３】

送信者と受信者とが、暗号通信を行なうための鍵を共有する鍵共有方法であって，

（１）鍵情報生成のステップとして，

【数４３】

- p, q:prime numbers
- $s \in \mathbf{Z}$ $(gh^s \equiv 1 \pmod{pq})$

$\cdots (数43)$

なる秘密鍵（p,q,s）を作成し，さらに，

【数４４】

- $g, h, k \in \mathbf{Z}$ $(0 < g, h < n)$
- $n = p^d q$ $(d \geq 1)$
- f : one-way function

$\cdots (数44)$

なる公開鍵（n,g,h,k,f）を作成し（但し，kはp,qのビット長），

（２）送信者は，前記公開鍵（n,g,h,k）を用いて，乱数r（$0<r<2^{k-1}$）を選び，送信データm（$0<m<2^{k-1}$）について，暗号文C,Dを，

【数４５】

$$C = m^2 g^r \bmod n, \qquad \cdots (数45)$$
$$D = h^r \bmod n$$

にて計算し，共有鍵KをK=f(m)により計算し，前記計算結果C,Dを前記受信者に送信し，

（３）前記受信者は，前記秘密鍵（p,q,s）を用いて，

【数４６】

$$m^2 = CD^s \bmod pq, \qquad \cdots (数46)$$

を計算し，前記送信データmを求め，前記公開情報ｆを用いて前記共有鍵KをK=f(m)により計算する

ことを特徴とする鍵共有方法。

【請求項１４】

請求項12において，

前記送信者は，前記送信データm（0<m<n）に対して，前記暗号化方法にて前記暗号文C,Dを作成し，前記暗号文C,Dを受信者に送信し，

前記受信者は，

【数４７】

$$m^2 = CD^s \bmod n, \qquad \cdots (数47)$$

を計算し，前記送信データmの復号化を行う

ことを特徴とする公開鍵暗号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は，公開鍵暗号を用いた暗号通信方法および装置に関する。

【０００２】

【従来の技術】

現在まで，様々な公開鍵暗号方式が提案されている。なかでも，

文献１「R. L. Rivest, A. Shamir, L. Adleman. :A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, Vol.21, No.2, pp.120-126, 1987.」
に記載されている方法が最も有名であり，最も実用化されている公開鍵暗号である。その他には，
文献２「T.ElGamal.:A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans. On Information Theory, IT-31, 4, pp.469-472(1985)」
に記載されている暗号方法，
文献３「M.O.Rabin.: Digital Signatures and Public-Key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCS/TR-212 (1979)」に記載されている暗号方法，
文献４「V. S. Miller. :Use of Elliptic Curves in Cryptography, Proc. of Crypto'85, LNCS 218, Springer - Verlag, pp.417-426 (1985)」，
文献５「N. Koblitz.: Elliptic Curve Cryptosystems, Math. Comp., 48, 177, pp.203-209 (1987)」
等に記載の楕円曲線を用いた暗号方法，
文献６「S. Goldwasser and S.Micali.: Probabilistic Encryption, JCSS, 28, 2, pp.270-299 (1984) 」に記載されている暗号方法，
文献７「M.Blum and S.Goldwasser.: An Efficient probabilistic public-key encryption scheme which hides all partial information, Proc. of Crypto'84, LNCS 196, Springer - Verlag, pp.289-299 (1985)」に記載されている暗号方法，
文献８「S.Goldwasser and M.Bellare.: Lecture Notes on Cryptography, http:/www-cse.ucsd.edu/users/mihir/ (1997)」に記載されている暗号方法，
文献９「R. Cramer and V. Shoup.: A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack, Proc. of Crypto98, LNCS, Springer - Verlag, pp.13-25 (1998)」に記載されている暗号方法，
などが知られている。最近では，

文献10「T. Okamoto and S. Uchiyama,. A New Public-Key Cryptosystem as Secure as Factoring, Proc. of Eurocrypt'98, LNCS, Springer Verlag, pp.308-318 (1998)」
の中で素因数分解問題の困難性と等価な（完全解読に対する）安全性を主張する公開鍵暗号方式が提案されている。

【０００３】

【発明が解決しようとする課題】

文献1に開示されている暗号方法の安全性は，素因数分解問題の困難性を仮定しているが，等価性は示されていない。すなわち，素因数分解問題を解ければ文献1の暗号方法を破ることできるが，逆は証明されていない。素因数分解問題よりも簡単な問題を解くことで文献1の暗号方法を破ることが出来る可能性は残されている。

【０００４】

さらに文献1の暗号方法は，確定的な暗号であるため、鍵が同一である場合，同一の平文に対する暗号文は常に同一になる。そのままで使用すると，複数の暗号文から平文の同一性を判断することが可能になるので、これを防ぐためには運用時は乱数情報を付加するという別処理が必要になり、効率が悪い。

【０００５】

これに対して，文献10に開示されている暗号方法では，受動的攻撃に対して暗号文から平文を求めること（完全解読）は素因数分解問題の困難性と等価であることが証明されており，これにより安全性を保証している。さらに，同一の平文であっても暗号文が変化する確率暗号であるため，文献1の暗号方法のような問題や、別処理の必要性はない。

【０００６】

また、文献10の暗号方法における部分解読に対する安全性（semantic security）は，文献10中にて定義されているp-部分群問題の困難性と等価であるとして、その安全性が主張されている。しかしながら、この問題は未だ十分な議論がなされておらず，その困難性については知られていない。つまり，p-部分群問題を解く効率的なアルゴリズムが見つかれば，文献10の暗号方法の部分解読を効率的

に行うことが出来てしまい、その安全性は保証できなくなる。

【０００７】

一般に，暗号の安全性を保証するためには，素因数分解問題や離散対数問題など計算量的困難性について十分議論されている問題との等価性を示すことが望ましい。

【０００８】

また、文献９に記載の暗号方法は、文献２に記載の暗号方法を用いて作成した暗号文に、暗号前のメッセージを知らないと作成できない「メッセージ情報」を付与するものである。このメッセージ情報が暗号文に対応する場合だけ正当な暗号文として対処し，そうでない場合は拒否するという仕組みであり、このメッセージ情報処理の処理量が多い。。

【０００９】

一方、携帯型情報処理機器の普及やネットワーク環境の発展などにより、これら携帯型情報処理機器を用いて電子商取引を行うことが増えてくると予想されている。これら情報機器においては、計算能力が限られている反面、電子商取引では、複雑なプロトコルのために、元々データ量が多い。したがって、暗号化に伴うデータ量を減らすよりは、計算負荷を減らす方が望まれる場合がある。

【００１０】

本発明の目的は，計算量的にその解決の困難性が予測されている数学的問題と等価な（または以上の）安全性を持つ、すなわち、安全性が保証された、公開鍵を用いた暗号化方法と復号化方法と、それを用いた鍵配送方法や鍵共有方法、さらには、それぞれの方法を実行するプログラム、装置またはシステムを提供することである。

【００１１】

また、本発明のより具体的な目的は、受動的攻撃による解読の困難性が，計算量的困難性が予想されている数論的問題(NP問題)と等価（または以上）であり、安全性が保証された公開鍵を用いた暗号化方法と復号化方法と、それを用いた鍵配送方法や鍵共有方法、さらには、これらの方法を実行するプログラム、装置またはシステムを提供することである。

【００１２】

本発明の他の目的は、上記、安全性が保証された暗号方法を用いて、能動的な攻撃方法である選択暗号文攻撃を許さない環境を提供し、あらゆる攻撃に対して安全性を確保することである。

【００１３】

本発明の他の目的は、上記、安全性が保証された暗号方法において、確率的暗号方法を提供することである。

【００１４】

また、本発明の他の目的は、計算負荷が小さく、携帯型情報処理機器など計算能力が限られた装置であっても高速処理が可能な、公開鍵を用いた暗号化方法と復号化方法と、それを用いた鍵配送方法や鍵共有方法、さらには、それぞれの方法を実行するプログラム、装置またはシステムを提供することである。

【００１５】

【課題を解決するための手段】

上記目的を達成するため、本発明は、以下の特徴を備える。

【００１６】

（１）受動的攻撃、より具体的には、公開鍵暗号における既知平文攻撃、選択平文攻撃や暗号文攻撃、のもとでの、暗号文から平文を求める完全解読は、素因数分解問題を解くよりも困難である。これにより，本発明が提供する暗号方法への、全文解読を目的とする受動的攻撃に対する安全性を，素因数分解問題の困難性を根拠とする従来の暗号方法よりもさらに強く保証する。

【００１７】

（２）受動的攻撃の元での部分解読の困難性は、Diffie-Hellman決定問題の困難性と等価である（Diffie-Hellman決定問題の困難性については，文献11「V.Shoup.: Lower bounds for discrete logarithms and related problems. In Advances in Cryptology-Eurocrypt'97 (1997)」において，その困難性が予想されている）。

【００１８】

これによって、本発明が提供する暗号化方法への部分解読を目的とする受動的

攻撃に対する安全性が保証される。さらに部分解読攻撃に対する安全性を保証されれば、完全解読攻撃に対する安全性もまた保証される。

【００１９】

（３）暗号化の過程において、確率的な情報を用いた処理を施す。これにより、暗号化する平文に対して確率的情報を挿入する必要がない。すなわち、本発明が提供する暗号化方法は、同一の平文であっても，暗号文の値が変化する確率暗号である。

【００２０】

（４）暗号化処理を行う者（以下、暗号化者という）および復号化処理を行う者（以下、復号化者という）の計算負荷が小さく，高速な処理が可能である。

【００２１】

（５）本発明が提供する暗号化方法に、実用的な一方向性関数を組み合わせ、能動的な攻撃方法である選択暗号文攻撃を許さない環境を作ることで、その安全性を確保する。

【００２２】

具体的には、本発明が提供する方法は、以下のステップから成るものであり、また、本発明が提供する装置は、以下のステップを実行する手段またはプログラムを備えるものである。

【００２３】

[鍵情報生成]

秘密鍵として，

【００２４】

【数４８】

- p, q:prime numbers
- $s \in \mathbf{Z}$ $(gh^s \equiv 1 \pmod{n})$

・・・(数４８)

【００２５】

公開鍵として，

【００２６】

【数４９】

- $g,h,k \in \mathbf{Z}\ (0 < g,h < n)$
- $n = p^d q\ (d \geq 1)$

・・・(数49)

【００２７】

を作成する（但し，Ｌはｇの位数，ｋはp,qのビット長を表す）。

【００２８】

[暗号化]

送信者は，乱数r（$0<r<2^{k-1}$）を選び，送信データｍ（$0<m<2^{k-1}$）を，

【００２９】

【数５０】

$$C = m^2 g^r \bmod n,$$
$$D = h^r \bmod n$$

・・・(数50)

【００３０】

により，暗号化する。さらに，送信者は暗号文Ｃ，Ｄを受信者に送信する。

【００３１】

[復号化]

受信者は，

【００３２】

【数５１】

$$m^2 = CD^s \bmod pq,$$

・・・(数51)

【００３３】

により，送信データｍを復号化する。

【００３４】

【発明の実施の形態】

以下，図面を用いて，本発明の実施例について説明する。

【００３５】

なお、本明細書においては、上記暗号化者を送信者、復号化者を受信者、暗号化の対象となる平文データｍを送信データｍともいう。

【００３６】

図１は，本発明の各実施例を実現するシステム構成を示す図である。

【００３７】

図１において、ネットワーク300に暗号化者が使用するコンピュータ（以下、暗号化者側装置、または送信者側装置ともいう）100、および、復号化者が使用するコンピュータ（以下、復号化者側装置、または受信者側装置ともいう）200、および、第３者が使用するコンピュータ（以下、第３者側装置ともいう）400が接続されている。

【００３８】

暗号化者側装置100は、CPU101、メモリ102、通信装置103、バス104によって構成され、さらにディスプレイ106、および、キーボード107がバス104に接続されている。

【００３９】

暗号化者側装置100のメモリ102は、メモリ102は半導体記憶装置やハードディスクなどの二次記憶装置で構成されるものであり、以下の各実施例に示す、各種情報と、CPU101が実行するプログラム（手段という）と、キーボード107や可搬型記憶媒体または通信回線300を介して入力される、暗号化の対象となる平文データ（送信データ）と、送信される暗号文が保存される。

【００４０】

同様に、復号化者側装置200には、CPU201、メモリ202、通信装置203、バス204によって構成され、さらにディスプレイ206、キーボード207、および、復号化者の所有する、ICカードと通信をすることができるICカードリーダ・ライタ205がバス204に接続されている。

【００４１】

復号化者側装置200のメモリ202は、半導体記憶装置やハードディスクなどの二次記憶装置で構成されるものであり、以下の各実施例に示す、各種情報と、CPU201が実行するプログラム（手段という）と、復号化の対象となる暗号文と、復号化され、ディスプレイ206や通信回線300に出力される平文データ（送信データ）が保存される。

【００４２】

（実施例 1）

本実施例は，メッセージの送信者Ａが受信者Ｂに対して，送信データｍ（0<m<2^{k-1}）を暗号通信によって送信する場合について説明する。

【００４３】

１．鍵情報生成処理

予め，受信者側装置200内の鍵生成手段2001は，

【００４４】

【数５２】

- p, q:prime numbers　　・・・(数52)
- $s \in \mathbf{Z}\ (gh^s \equiv 1 \pmod{p})$

【００４５】

なる秘密情報（p,q,s）を作成し，

【００４６】

【数５３】

- g, h, $k \in \mathbf{Z}\ (0 < g, h < n)$　　・・・(数53)
- $n = p^d q \quad (d \geq 1)$

【００４７】

なる公開情報（n,g,h,k）（但し，ｋはｐ，ｑのビット長を表す。）を作成する。

【００４８】

そして上記公開情報2006を通信回線300などを介して出力し、送信者側装置100へ送付するか、または公開する。公開する方法として、たとえば公開情報管理機関（たとえば第3者側装置400）への登録など、周知の方法を用いることが可能である。上記秘密情報2007は、メモリ202に格納する。

【００４９】

２．暗復号化処理

（１）送信者側装置100内の暗号化手段1004は、乱数生成手段1001を用いて、整数r（$0<r<2^{k-1}$）をランダムに選ぶ。さらに、第3者装置400あるいは、受信者側装置200から得られる上記公開情報2006と，べき乗算手段1002，剰余演算手段1003とを用いて，送信データm（$0<m<2^{k-1}$）に対する暗号文Ｃ，Ｄを

【００５０】

【数５４】

$$C = mg^r \bmod n, \qquad \cdots(数54)$$
$$D = h^r \bmod n$$

【００５１】

にて計算する。

【００５２】

さらに，暗号文Ｃ，Ｄを、通信装置103を用いて通信回線300を介して受信者Ｂの受信者側装置200に送信する。

【００５３】

（２）受信者側装置200において，復号化手段2004は、べき乗算手段2002，剰余演算手段2003と、保持されている上記秘密情報2007とを用いて，

【００５４】

【数５５】

$$m = CD^s \bmod p, \qquad \cdots(数55)$$

【００５５】

にて，暗号文Ｃ，Ｄから送信データｍを復号化する。

【００５６】

上記文献９では、文献２に記載の暗号方法において，semantic securityがDiffie - Hellman決定問題の困難性のもとで示すことができると、指摘されている。これと同様にして，本実施例の方法を用いれば、受動的な暗号文攻撃に対して、平文の部分情報(少なくとも任意の1ビット)を求める部分解読がDiffie - Hellman決定問題と同等に困難であること、すなわち、本発明の方法は、Semantically secureであることを証明することが出来る。

【００５７】

なお、Diffie-Hellman決定問題とは，

【００５８】

【数５６】

$$R : (g^x \bmod n, g^y \bmod n, g^z \bmod n) \quad g, x, y, z \text{ are random} \qquad \cdots (数56)$$

【００５９】

からのシーケンスと

【００６０】

【数５７】

$$D : (g^x \bmod n, g^y \bmod n, g^{xy} \bmod n) \quad g, x, y, z \text{ are random} \qquad \cdots (数57)$$

【００６１】

からのシーケンスのいずれか一方がランダムに与えられたとき，どちらからのシーケンスかを言い当てる問題である。

【００６２】

本実施例による方法では，適当な秘密の整数αに対して，

【００６３】

【数５８】

$$h \equiv g^{\alpha} \pmod{n} \qquad \cdots(数58)$$

【００６４】

と書けるとき，g，α，m0,m1をランダムに選ぶと，

【００６５】

【数５９】

$$(C/m_i \bmod n, h, D) \quad (0 \leq i \leq 1) \qquad \cdots(数59)$$

【００６６】

なるシーケンスはそれぞれＲおよびＤの分布を示す（但し，暗号文C,Dはm0かm1のどちらかの暗号文）。このとき，本実施例の方法に対して部分解読を行う問題は，このDiffie-Hellman決定問題を解くことと同値であることが示される。

【００６７】

これにより，部分解読の困難性とDiffie-Hellman決定問題の困難性とが等価であることにより、その安全性を保証することができる。さらに、部分解読に対する安全性を保証することができるため、完全解読に対する安全性も、同じく保証することができる。

【００６８】

以上述べたように、本発明の方法は、受動的攻撃に対する安全性を保証することができる。

【００６９】

また、後述するように、本発明による暗号化、復号化方法は、モジュラー積の個数という観点からみて非常に効率がよいことがわかる。

さらに、送信者側において、暗号化処理の際，乱数rが導入されているため，本発明の方法は，確定的ではなく，確率的である。よって，新たに乱数情報を含ませることなく，暗号文から平文の同一性を判断することは困難であり，文献１の方法などと比較して安全性を向上させている。言い換えると、安全性を向上さ

せるために乱数情報を新たに含ませる必要がなく、運用時の処理を簡単にすることができる。

【００７０】

なお、上記公開情報は、必ずしも受信者が作成する必要はなく、システム構成によっては、管理者である第3者が作成して、システム参加者へ配布してもよいものである。

【００７１】

（実施例 2）

本実施例は、上記実施例１で述べた方法に、さらに、実用的な一方向性関数を組み合わせるものである。これにより、送信者と受信者の間で鍵共有を行うこと（すなわち、共通鍵暗号方法に用いる鍵を配送すること）を可能にする。また、能動的な攻撃方法である選択暗号文攻撃を許さない環境を作り、能動的攻撃に対する安全性を確保する。

【００７２】

本実施例では、図１のシステム構成において、図２に示すICカード500を、受信者側装置200のICカードリーダライタ205に挿入して用いる。このとき、受信者側装置200の復号化手段2004、べき乗算手段2002，剰余演算手段2003はなくてもよい。

また、一方向性関数手段2008を新たに送信者側装置100内に設ける。

また、配送された（または共有する）鍵を用いて、同時に、あるいは別途送受するデータを、おのおの暗号化、復号化する機能を有するアプリケーションAプログラム1005、アプリケーションBプログラム2005を、図1に示すように備えるものとする。

【００７３】

１．鍵情報生成処理

予め，受信者側装置200内の鍵生成手段2001は，

【００７４】

【数６０】

- p, q:prime numbers
- $s \in \mathbf{Z}\ (gh^s \equiv 1 \pmod{p})$

・・・(数60)

【００７５】

なる秘密情報（p,q,s）を作成し，

【００７６】

【数６１】

- g, h, $k \in \mathbf{Z}\ (0 < g, h < n)$
- $n = p^d q \quad (d \geq 1)$
- f : one-way function

・・・(数61)

【００７７】

なる公開情報（n,g,h,k）（但し，ｋはｐ，ｑのビット長を表す。）を作成する。

【００７８】

そして、公開情報としてn,g,h,kを通信回線300などを介して出力し、受信者側装置200へ送付するか、または公開する。公開する方法として、たとえば公開情報管理機関（たとえば第3者側装置400）への登録など、周知の方法を用いることが可能である。その他の情報は、メモリ202に格納する。

【００７９】

２．暗復号化処理

（１）送信者側装置100内の暗号化手段1004は、乱数生成手段1001を用いて整数r（$0<r<2^{k-1}$）をランダムに選び，公開情報2006、べき乗算手段1002，剰余演算手段1003を用いて，送信データｍ（$0<m<2^{k-1}$）に対する暗号文Ｃ，Ｄを

【００８０】

【数６２】

$$C = mg^r \bmod n,$$
$$D = h^r \bmod n \qquad \cdots(数62)$$

【００８１】

にて計算する。

【００８２】

さらに，暗号文Ｃ，Ｄを通信装置103を用いて通信回線300を介して受信者Ｂの受信者側装置200に送信する。

【００８３】

さらに、送信者側装置100内の一方向性関数手段2008は、公開情報である一方向性関数ｆから共通鍵Ｋを$K=f(m)$により計算する。必要に応じて、アプリケーションAプログラム1005は、共通鍵Kを用いて暗号化計算を行う。

【００８４】

（２）受信者側装置200では，ICカード500内の復号化手段5004が、メモリ502に保持されている上記秘密情報2007と、べき乗算手段5002，剰余演算手段5003とを用いて，

【００８５】

【数６３】

$$m = CD^s \bmod p, \qquad \cdots(数63)$$

【００８６】

にて，暗号文Ｃ，Ｄから送信データｍを復号化する。

【００８７】

さらに，ICカード500内の一方向性関数手段5008は，公開情報である一方向性関数ｆから共通鍵Ｋを$K=f(m)$により計算し、ICカード500からｍを出力することなく、Kを受信者側装置200に出力する。

【００８８】

受信者側装置200内のアプリケーションBプログラム2005は、この共通鍵Kを用いて、同時に、あるいは、別途送付される、共通鍵Kで暗号化されたデータを復号化する。

【００８９】

上述のように，本実施例は，実用的な一方向性関数を組み合わせて使用することにより、平文データm（$0<m<2^{k-1}$）を外部へ出力しない。

【００９０】

このように、ICカード(または、計算機カード)など個人が携帯する周辺機器内部で、暗号化、復号化処理を行うことで、選択暗号文攻撃を許さない、すなわち能動的攻撃に対しても安全な環境を作ることができる。

【００９１】

また，メッセージそのものを、本発明による公開鍵暗号方法を用いて送信する構成においては，本実施例のアプリケーションBプログラム2005が、復号化したメッセージ（平文データｍ）を所定の知識/ルールによって解釈して、意味のないメッセージが復号化されたと判断した場合，そのメッセージを秘密のうちに消去するなどして、他に知れないようにすることで，能動的攻撃を許さない環境を作ることが出来る。

【００９２】

上述のように，本実施例は，実用的な一方向性関数を組み合わせて使用することにより、さらに、能動的攻撃に対しても安全な環境を作るものである。

【００９３】

（実施例 3）

本実施例は，実施例１および実施例2において，送信者の計算効率を高めるための鍵情報生成の方法について述べる。

【００９４】

受信者側装置200内の鍵生成手段2001は，有限群$G=\{x\in Z/(n)\mid x$は可逆元$\}$の大きな位数Ｌを持つ元ξを選び（但し，$Z/(n)$はnを法とする剰余環，Ｌはξの位数の倍数でもよい），整数α，βに対して，

【００９５】

【数６４】

$$g = \xi^{\alpha} \bmod n, \qquad h = \xi^{\beta} \bmod n \qquad \cdots (数64)$$

【００９６】

とする。さらに，

【００９７】

【数６５】

$$\alpha + s\beta \equiv 0 \pmod{L} \qquad \cdots (数65)$$

【００９８】

となるようにｓを決める。

【００９９】

このとき，ｇ，ｈにおいて，小さな整数ｋ（ｋ≧２）に対して

【０１００】

【数６６】

$$h = g^{k} \bmod n \qquad \cdots (数66)$$

【０１０１】

とすると，送信者側の計算効率をさらに高めることができる。

【０１０２】

ここで，小さな整数kを選ぶことは，kを公開情報にすることに等しくなり、部分解読に対する安全性とDiffie-Hellman決定問題の困難性との等価性への保証がなくなることがある。しかし、これは、部分解読に対して弱いということを意味するものではない。

【０１０３】

また，公開鍵g,hが小さな値となるようにp,q,ξ,α,βを選ぶことにより，公開鍵のサイズを小さくすることが可能である。より具体的には，ｇを大きな奇数（例えば素数）Ｌを位数とする小さな値を選び，

【０１０４】

【数６７】

$$h = g^2 \bmod n \qquad \cdots(数67)$$

【０１０５】

とする。さらに，

【０１０６】

【数６８】

$$2s + 1 \equiv 0 \pmod{L} \qquad \cdots(数68)$$

【０１０７】

にてｓを計算する。

【０１０８】

送信者側装置100内の暗号化手段1004は，べき乗算手段1002，剰余演算手段1003を用いて，

【０１０９】

【数６９】

$$W = g^r \bmod n \qquad \cdots(数69)$$

【０１１０】

を計算し，さらに，

【０１１１】

【数７０】

$$C = mW \bmod n, \quad D = W^2 \bmod n \qquad \cdots(数70)$$

【０１１２】

により暗号文を計算することで，送信者側装置の計算負担を少なくすることが出来る（図4）。

【０１１３】

また，ｄ（ｄ≧１）の値をｎの素因数分解が困難である範囲において，大きく選ぶことで，ｎのビット数が一定の場合，ｐのビット数が小さくなるため，復号化処理を高速に行うことが出来る。このｄの値を、第3者側装置400あるいは、受信者側装置200にて管理すれば、計算機能力の発展、素因数分解に必要とされる計算時間と安全性との関係などによって、変えることが可能である。

【０１１４】

図５に，代表的な実用的公開鍵暗号方法（それぞれの方法については，従来の技術の項にて述べた上記各文献に記載されている）とのモジュラー積の個数による効率性の比較を示す。ここにあるデータの従来方式に関するものは文献10から引用したものであり，また，本発明による方式では，文献10にて提案されている暗号方法と同様の底となるようにd=2としている。

【０１１５】

なお、図5に示す本発明による効率は、送信側より受信側の方が、負荷が少ないが、送信側では後述するように、送信データを用いない計算部分を、前処理とすることが可能である。この結果、送信側の効率も大幅に向上させることができる。

【０１１６】

（実施例 4）

本実施例は実施例１の変形例である。

本実施例では，実施例１に対して，nを法とした剰余環の上で復号化を行うことにより，送信データｍを長くすることを可能とし、また、選択暗号文攻撃に対する対策を行っている。

【０１１７】

１．鍵情報生成処理

予め，受信者側装置200内の鍵生成手段2001は，

【０１１８】

【数７１】

- p, q:prime numbers
- $s \in \mathbf{Z}\ (gh^s \equiv 1 \pmod{n})$

・・・(数71)

【０１１９】

なる秘密情報（p,q,s）を作成し，

【０１２０】

【数７２】

- g, h, $k \in \mathbf{Z}\ (0 < g, h < n)$
- $n = pq$

・・・(数72)

【０１２１】

なる公開情報（n,g,h,k）（但し，ｋはｐ，ｑのビット長を表す。）を作成する。

【０１２２】

受信者Bは、公開情報としてn,g,h,kを通信回線300などを介して出力し、受信者側装置200へ送付するか、または公開する。公開する方法として、たとえば公開情報管理機関（たとえば第3者側装置400）への登録など、周知の方法を用いることが可能である。その他の情報は、メモリ202に格納する。

【０１２３】

２．暗復号化処理

（１）送信者側装置内の暗号化手段1004は、乱数生成手段1001を用いて整数r（$0<r<2^{k-1}$）をランダムに選ぶ。さらに、第3者あるいは、受信者側装置200から得られる上記公開情報2006と、べき乗算手段1002，剰余演算手段1003とを用いて，送信データmに対する暗号文Ｃ，Ｄを

【０１２４】

【数７３】

$$C = mg^r \bmod n,$$
$$D = h^r \bmod n$$

・・・(数73)

【０１２５】

にて計算する。

【０１２６】

さらに，暗号文Ｃ，Ｄを通信装置103を用いて通信回線300を介して受信者Ｂの受信者側装置200に送信する。

【０１２７】

（２）受信者側装置200において，復号化手段2004は、べき乗算手段2002，剰余演算手段2003と、保持されている上記秘密情報2007とを用いて，

【０１２８】

【数７４】

$$m = CD^s \bmod n, \qquad \cdots(数74)$$

【０１２９】

にて，暗号文Ｃ，Ｄから送信データｍを復号化する。

（実施例 5）

本実施例は，実施例４において，送信者の計算効率を高めるための鍵生成の方法について述べる。

【０１３０】

受信者側装置200内の鍵生成手段201は，有限群G=｛x∈Z/(n)｜xは可逆元｝の大きな位数Ｌを持つ元ξを選び（但し，Z/(n)はnを法とする剰余環，Ｌはξの位数の倍数でもよい），整数α，βに対して，

【０１３１】

【数７５】

$$g = \xi^{\alpha} \bmod n, \quad h = \xi^{\beta} \bmod n \qquad \cdots(数75)$$

【０１３２】

とする。さらに，

【０１３３】

【数７６】

$$\alpha + s\beta \equiv 0 \pmod{L} \qquad \cdots (数76)$$

【０１３４】

となるようにｓを決める。

【０１３５】

このとき，ｇ，ｈにおいて，小さな整数ｋ（ｋ≧２）に対して

【０１３６】

【数７７】

$$h = g^k \bmod n \qquad \cdots (数77)$$

【０１３７】

とすると，送信者側の計算効率をさらに高めることができる。

【０１３８】

また，公開鍵g,hが小さな値となるようにp,q,ξ,α,βを選ぶことにより，公開鍵のサイズを小さくすることが可能である。

【０１３９】

より具体的には，ξを大きな奇数（例えば素数）Ｌを位数とする小さな値を選び，α＝１，β＝２とする。このとき，

【０１４０】

【数７８】

$$h = g^2 \bmod n \qquad \cdots (数78)$$

【０１４１】

となり，送信者側装置100内の暗号化手段1004は，べき乗算手段1002，剰余演算手段1003を用いて，

【０１４２】

【数７９】

$$W = g^r \bmod n \qquad \cdots(数79)$$

【０１４３】

を計算し，さらに，

【０１４４】

【数８０】

$$C = mW \bmod n, \qquad D = W^2 \bmod n \qquad \cdots(数80)$$

【０１４５】

により暗号文を計算することで，送信者側装置の計算負担を少なくすることが出来る。

【０１４６】

（実施例 6）

本実施例は，実施例４において，受信者の計算効率を高めるための復号化方法について述べる。図6は本実施例の概要を示す。

【０１４７】

受信者側装置200において、復号化手段2004は、べき乗算手段2002，剰余演算手段2003と、保持されている上記秘密情報2007とを用いて，

【０１４８】

【数８１】

$$m_1 = CD^s \bmod p, \qquad m_2 = CD^s \bmod q \qquad \cdots(数81)$$

【０１４９】

を計算し，さらに

【０１５０】

【数８２】

$$a \equiv 1 \pmod{p}, \quad a \equiv 0 \pmod{q}, \quad b \equiv 0 \pmod{p}, \quad b \equiv 1 \pmod{q} \qquad \cdots (数82)$$

【０１５１】

なる整数ａ，ｂに対して，

【０１５２】

【数８３】

$$m = am_1 + bm_2 \bmod n \qquad \cdots (数83)$$

【０１５３】

にて，暗号文Ｃ，Ｄから送信データｍを復号化する。

【０１５４】

（実施例 7）

上記各実施例において，

【０１５５】

【数８４】

$$g^r \bmod n, \quad h^r \bmod n \qquad \cdots (数84)$$

【０１５６】

の計算は暗号化対象である平文データｍに関係しないため，前処理が可能である。すなわち、送信者側装置100において、この計算を前処理として行い、その結果を上記メモリ102に保存しておき、平文データｍを暗号化する時にその値を読み出して用いると、データｍを用いた処理のモジュラー積の個数は1個となるため，暗号化時間を、さらに大幅に短縮する事が出来る。

【０１５７】

（実施例 8）

本実施例は，実施例１の変形例である。本実施例は，実施例3と同様に、送信者側の計算効率の向上を図るものである。

【０１５８】

１．鍵生成処理

予め，受信者側装置200内の鍵生成手段2001は，

【０１５９】

【数８５】

- p, q:prime numbers ・・・(数85)
- $s_0, s_1 \in \mathbf{Z}$

【０１６０】

なる秘密情報（p,q,s0,s1）を作成し，

【０１６１】

【数８６】

- $g, h, k \in \mathbf{Z}\ (0 < g, h < n)$ ・・・(数86)
- $n = p^d q\ (d \geq 1)$

【０１６２】

なる公開情報（n,g,h,k）

（但し，ｋはｐ，ｑのビット長を表す。また，ｓｉ（ｉ=1,2）は，

【０１６３】

【数８７】

$$s_i \alpha_i + \beta \equiv 0 \pmod{L} \quad (0 \leq i \leq 1)$$ ・・・(数87)

【０１６４】

なる関係を満たす。）を作成する。

【０１６５】

そして、上記公開情報を通信回線300などを介して出力し，送信者側装置100へ送付するか，または公開する。公開する方法として，例えば公開情報管理機関（たとえば第3者側装置400）への登録など，周知の方法を用いることが可能である。その他の情報については，メモリ202に格納する。

【０１６６】

２．暗復号化処理

（１）送信者側装置100内の暗号化手段1004は、乱数生成手段1001を用いて、整数r（$0<r<2^{k-1}$）をランダムに選ぶ。さらに、送信データm（$0<m<2^{k-1}$）についてm=m0+m1となるようにランダムにm0,m1を選ぶ。さらに，第3者側装置400あるいは受信者側装置200から得られる上記公開情報2006と，べき乗算手段1002，剰余演算手段1003を用いて，送信データmに対する暗号文C0,C1,Dを

【０１６７】

【数８８】

$$C_0 = m_0 g^{\alpha_0 r} \bmod n,$$
$$C_1 = m_1 g^{\alpha_1 r} \bmod n, \qquad \cdots (数88)$$
$$D = g^{\beta r} \bmod n,$$

【０１６８】

にて計算する。

【０１６９】

さらに，暗号文C0,C1,Dを通信装置103を用いて通信回線300を介して受信者Ｂの受信者側装置200に送信する。

【０１７０】

（２）受信者側装置200において、復号化手段2004は、保持している上記秘密情報2007と，べき乗算手段2002，剰余演算手段2003とを用いて，

【０１７１】

【数８９】

$$m = C_0 D^{s_0} + C_1 D^{s_1} \bmod p \qquad \cdots (数89)$$

【０１７２】

にて，暗号文C0,C1,Dから送信データｍを復号化する。

【０１７３】

また，送信者は暗号化処理の際，乱数rを導入しているため，本発明の方法は，確定的ではなく，確率的である。よって，新たに乱数情報を含ませることなく

，暗号文から平文の同一性を判断することは困難であり，文献１の方法などと比較して安全性を向上させている。

【０１７４】

（実施例 9）

本実施例は，上記実施例で述べた方法に，一方向性関数を組み合わせるものである。これにより，送信者と受信者の間で鍵共有を行うこと(すなわち、共通鍵暗号方法に用いる鍵を配送すること)を可能にする。また、能動的な攻撃方法である選択暗号文攻撃を許さない環境を作り、能動的攻撃に対する安全性を確保する。

【０１７５】

１．鍵生成処理

予め，受信者側装置200内の鍵生成手段2001は，

【０１７６】

【数９０】

- p, q:prime numbers
- $s_0, s_1 \in \mathbf{Z}$

・・・(数９０)

【０１７７】

なる秘密情報（p,q,s0,s1）を作成し，

【０１７８】

【数９１】

- $g, h, k \in \mathbf{Z}\ (0 < g, h < n)$
- $n = p^d q\ (d \geq 1)$
- f : one-way function

・・・(数９１)

【０１７９】

なる公開情報（n,g,h,k,f）

（但し，ｋはｐ，ｑのビット長を表す。また，si（i=1,2）は，

【０１８０】

【数９２】

$$s_i\alpha_i+\beta\equiv 0 \pmod{L} \quad (0\leq i\leq 1) \qquad \cdots(数92)$$

【０１８１】

なる関係を満たす。）を作成する。

【０１８２】

そして、公開情報としてn,g,h,k,fを通信回線300などを介して出力し、受信者側装置200へ送付するか、または公開する。公開する方法として、たとえば公開情報管理機関（たとえば第3者側装置400）への登録など、周知の方法を用いることが可能である。その他の情報は、メモリ202に格納する。

【０１８３】

２．暗復号化処理

（１）送信者側装置100内の暗号化手段1004は、乱数生成手段1001を用いて整数r（$0<r<2^{k-1}$）をランダムに選ぶ。さらに，送信データm（$0<m<2^{k-1}$）についてm=m0+m1となるようにランダムにm0,m1を選ぶ。さらに，第3者側装置400あるいは受信者側装置200から得られる上記公開情報2006と、べき乗算手段1002，剰余演算手段1003を用いて，送信データmに対する暗号文C0,C1,Dを

【０１８４】

【数９３】

$$\begin{aligned} C_0 &= m_0 g^{\alpha_0 r} \bmod n, \\ C_1 &= m_1 g^{\alpha_1 r} \bmod n, \\ D &= g^{\beta r} \bmod n, \end{aligned} \qquad \cdots(数93)$$

【０１８５】

にて計算する。

【０１８６】

さらに，暗号文C0,C1,Dを通信装置103を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【０１８７】

さらに、送信者側装置100内の一方向性関数手段2008は、公開情報である一方向性関数ｆから共通鍵ＫをK=f(m)により計算する。必要に応じて、アプリケーションAプログラム1005は、共通鍵Kを用いて暗号化計算を行う。

【０１８８】

（２）受信者側装置200では、ICカード500内の復号化手段5004が、メモリ502に保持されている上記秘密情報2007と，べき乗算手段5002，剰余演算手段5003とを用いて，

【０１８９】

【数９４】

$$m = C_0 D^{s_0} + C_1 D^{s_1} \bmod p \qquad \cdots (数94)$$

【０１９０】

にて，暗号文C0,C1,Dから送信データｍを復号化する。

【０１９１】

さらに，ICカード500内の一方向性関数手段5008は、公開情報である一方向性関数ｆから共通鍵ＫをK=f(m)により計算し，ICカード500からｍを出力することなく、Kを受信者側装置200に出力する。

【０１９２】

受信者側装置200内のアプリケーションBプログラム2005は、この共通鍵Kを用いて、同時に、あるいは、別途送付される、共通鍵Kで暗号化されたデータを復号化する。

【０１９３】

上述のように，本実施例は，実用的な一方向性関数を組み合わせて使用することにより、平文データｍ（$0<m<2^{k-1}$）を外部へ出力しない。

【０１９４】

このように、ICカード(または、計算機カード)など個人が携帯する周辺機器内部で、暗号化、復号化処理を行うことで、選択暗号文攻撃を許さない、能動的攻撃に対しても安全な環境を作ることができる。

【０１９５】

また，メッセージそのものを本発明による公開鍵暗号方法を用いて送信する構成においては，本実施例のアプリケーションBプログラム2005が、復号化したメッセージ（平文データｍ）を所定の知識/ルールによって解釈して、意味のないメッセージが復号化されたと判断した場合，そのメッセージを秘密のうちに消去するなどして、他に知れないようにすることで，能動的攻撃を許さない環境を作ることが出来る。

【０１９６】

上述のように，本実施例は，実用的な一方向性関数を組み合わせて使用することにより、さらに、能動的攻撃に対しても安全な環境を作るものである。

【０１９７】

（実施例10）

本実施例は実施例８のさらなる変形例である。

実施例８に示した暗号化方法において，送信者側装置100の暗号化手段1004は、送信データｍ（0<m<ｎ）に対して，暗号文(C0,C1,D)を作成する。

【０１９８】

受信者側装置200の復号化手段2004は、上記秘密情報2007と、べき乗算手段2002，剰余演算手段2003とを用いて，

【０１９９】

【数９５】

$$m = C_0 D^{s0} + C_1 D^{s1} \bmod n \qquad \cdots (数95)$$

【０２００】

にて，暗号文(C0,C1,D)から送信データｍを復号化する。

【０２０１】

本実施例では，送信データｍの範囲を実施例８に比べて広く取れるため，実施例８に比べて長いメッセージを送ることが可能である。

【０２０２】

（実施例 11）

実施例８および実施例９において，送信者側装置100の暗号化手段1004が、べき乗算手段1002，剰余演算手段1003を用いて，

【０２０３】

【数９６】

$$W = g^r \bmod n \qquad \cdots(数96)$$

【０２０４】

を計算し，さらに

【０２０５】

【数９７】

$$g^{\alpha_i r} \bmod n = W^{\alpha_i} \bmod n \quad (0 \le i \le 1), \qquad g^{\beta r} \bmod n = W^{\beta} \bmod n \qquad \cdots(数97)$$

【０２０６】

により，各々の値を計算することにより，効率的な暗号化処理が可能となる。

【０２０７】

（実施例 12）

実施例８および実施例１０において，

【０２０８】

【数９８】

$$g^{\alpha_i r} \bmod n \quad (0 \le i \le 1), \qquad g^{\beta r} \bmod n \qquad \cdots(数98)$$

【０２０９】

の計算は暗号化対象である平文データｍに関係しないため，前処理が可能である。すなわち、送信者側装置100において、この計算を前処理として行い、その結果を上記メモリ102に保存しておき、平文データｍを暗号化する時にその値を読み出して用いると、実施例7と同様に暗号化時間を、さらに大幅に短縮する事が出来る。

【０２１０】

（実施例13）

本実施例は，実施例１の変形例である。

【０２１１】

まず、本実施例の概念は、送信者が，受信者の公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって，

（１）鍵情報生成のステップとして，

【０２１２】

【数９９】

- $s \in \mathbf{Z}, \quad gh^s = 1 \ (\in H)$
- H: subgroup of G

・・・(数９９)

【０２１３】

なる前記秘密鍵（s,H）を作成し，さらに，

【０２１４】

【数１００】

- $g, h \in G$
- G : finite group

・・・(数１００)

【０２１５】

なる前記公開鍵（g,h,G）を作成し，

（２）前記送信者は，前記公開鍵（g,h,G）を用いて，乱数rを選び，前記送信データm（m∈H）について，暗号文C,Dを

【０２１６】

【数１０１】

$$C = m^t g^r \ (\in G),$$
$$D = h^r \ (\in G)$$

・・・(数１０１)

【０２１７】

にて計算し，該暗号文C,Dを前記受信者に送信し，

（３）前記受信者は，前記秘密鍵（s,H）を用いて，

【０２１８】

【数１０２】

$$m^t = CD^s \ (\in H), \qquad \cdots (数102)$$

【０２１９】

を計算し，これより前記送信データmを求めるものである。

【０２２０】

以下、具体的な実施例について説明する。

【０２２１】

１．鍵生成処理

受信者Ｂは，予め，受信者側装置200内の鍵生成手段2001を用いて，

【０２２２】

【数１０３】

- p, q:prime numbers
- $s \in \mathbf{Z}\ (gh^s \equiv 1 \pmod{pq})$

$\cdots (数103)$

【０２２３】

なる秘密情報（p,q,s）を作成し，

【０２２４】

【数１０４】

- $g, h, k \in \mathbf{Z}\ (0 < g, h < n)$
- $n = p^d q\ (d \geq 1)$

$\cdots (数104)$

【０２２５】

なる公開情報（n,g,h,k）を作成し（但し，ｋはｐ，ｑのビット長を表す。），公開情報を通信回線300などを介して出力し，送信者側装置100へ送付するか，または公開する。公開する方法として，例えば第３者（公開情報管理機関）への登録など，周知の方法を用いることが可能である。その他の情報については，メモリ202に格納する。

【０２２６】

２．暗復号化処理

（１）送信者Ａは，送信者側装置内の暗号化手段1004や乱数生成手段1001を用いて整数r（$0<r<2^{k-1}$）をランダムに選ぶ。さらに，第3者あるいは受信者Bから上記公開情報を得て，暗号化手段1004，べき乗算手段1002，剰余演算手段1003を用いて，送信データm（$0<m<2^{k-1}$）から，暗号文Ｃ，Ｄを

【０２２７】

【数１０５】

$$C = m^2 g^r \bmod n,$$
$$D = h^r \bmod n \qquad \cdots(数105)$$

【０２２８】

にて計算する。

【０２２９】

さらに，暗号文Ｃ，Ｄを通信装置103を用いて通信回線300を介して受信者Ｂの受信者側装置200に送信する。

【０２３０】

（２）受信者Ｂは，保持している上記秘密情報と，受信者側装置200内の復号化手段2004、べき乗算手段2002，剰余演算手段2003を用いて，

【０２３１】

【数１０６】

$$m^2 = CD^e \bmod pq, \qquad \cdots(数106)$$

【０２３２】

を計算し，これより送信データmを復号化する。ここで，mを計算する手段としては，文献３や文献「Berlekamp,E.R.:Factoring Polynomials over Finite Field, Bell. Sys. Tech. J. 46,pp.1853-1859 (1967)」による方法の他，nがBlum数の場合における簡単な計算方法，などが知られている。また，これらの方法により得られた複数解を一意的に選択する方法も幾つか知られている（文献「岡本，山本：現代暗号，産業図書」）。

【０２３３】

上記方法を用いれば，文献３にて開示されているものと同様の考察により，ある前提の下で，受動的攻撃に対して暗号文から平文を求めること（完全解読）は，ｎを素因数分解することよりも困難であることを証明することができる。

【０２３４】

証明のアウトラインについて以下に述べる。

【０２３５】

本実施例による方式が完全解読できたとすると，nの素因数分解ができることを示す。本実施例で述べた方法が破るアルゴリズムＩが存在したと仮定する。このとき，このアルゴリズムＩを利用してｎの素因数分解を行うアルゴリズムを次のように構成できる。ｃなるm'を選び，ランダムな整数r'に対し，暗号文(C',D')を，

【０２３６】

【数１０７】

$$C' = m'^2 g^{r'} \bmod n, \qquad \cdots(\text{数}107)$$
$$D' = h^{r'} \bmod n$$

【０２３７】

にて作成する。このとき，暗号文(C',D')をアルゴリズムＩに入力して，平文mを計算する。このとき，無視できない確率でm（または，m'）の範囲に複数の解が存在するとき，m-m'(≠0)とnの公約数を調べることにより，ｎの素因数分解を行うことが出来る。素因数分解問題はＮＰ問題であり，効率よく解くアルゴリズムは存在しないことが十分に議論された上で予想されているため，上記方法による暗号通信の安全性が保証することができる。

【０２３８】

また，上記方法を用いれば，semantic securityがDiffie-Hellman決定問題の困難性のもとで実施例１の場合と同様にして示すことができる。

【０２３９】

以上述べたように，本発明の方法は受動的攻撃に対する安全性を保証することができる。

【０２４０】

また，送信者は暗号化処理の際，乱数rを導入しているため，本発明の方法は，確定的ではなく，確率的である。よって，新たに乱数情報を含ませることなく，暗号文から平文の同一性を判断することは困難であり，文献１の方法などと比較して安全性を向上させている。

【０２４１】

（実施例 14）

本実施例は，上記実施例１３で述べた概念とその具体的な方法に対して，実施例２などと同様な一方向性関数を組み合わせるものである。これにより，送信者と受信者の間で鍵共有を行うこと（例えば，共通鍵暗号方法に用いる鍵の配送）を可能にする。また，能動的攻撃方法である選択暗号文攻撃を許さない環境を作り，能動的攻撃に対する安全性を確保する。

【０２４２】

１．鍵生成処理

受信者Ｂは，予め，受信者側装置200内の鍵生成手段2001を用いて，

【０２４３】

【数１０８】

- p, q:prime numbers
- $s \in \mathbf{Z}\ (gh^s \equiv 1 \pmod{pq})$

・・・(数１０８)

【０２４４】

なる秘密情報（p,q,s）を作成し，

【０２４５】

【数１０９】

- $g, h, k \in \mathbf{Z}\ (0 < g, h < n)$
- $n = p^d q\ (d \geq 1)$
- f : one-way function

・・・(数１０９)

【０２４６】

なる公開情報（n,g,h,k）を作成し（但し，ｋはｐ，ｑのビット長を表す。），公開情報を通信回線300などを介して出力し，送信者側装置100へ送付するか，ま

たは公開する。公開する方法として，例えば第３者（公開情報管理機関）への登録など，周知の方法を用いることが可能である。その他の情報については，メモリ202に格納する。

２．暗復号化処理

（１）送信者側装置100内の乱数生成手段1001を用いて整数r（$0<r<2^{k-1}$）をランダムに選ぶ。さらに，第3者あるいは受信者Bから上記公開情報を得て，暗号化手段1004、べき乗算手段1002，剰余演算手段1003を用いて，送信データm（$0<m<2^{k-1}$）から，暗号文Ｃ，Ｄを

【０２４７】

【数１１０】

$$C = m^2 g^r \bmod n,$$
$$D = h^r \bmod n \qquad \cdots(数110)$$

【０２４８】

にて計算する。

【０２４９】

さらに，暗号文Ｃ，Ｄを通信装置103を用いて通信回線300を介して受信者Ｂの受信者側装置200に送信する。

【０２５０】

送信者Ａは，送信者側装置100内の一方向性関数手段2008は、公開情報である一方向性関数ｆから共通鍵ＫをK=f(m)により計算する。

【０２５１】

（２）受信者Ｂは，ICカード500内にて保持している上記秘密情報2007と， ICカード500内の復号化手段5004、べき乗算手段5002，剰余演算手段5004を用いて，

【０２５２】

【数１１１】

$$m^2 = CD^s \bmod pq, \qquad \cdots(数111)$$

【０２５３】

を計算し，これより送信データｍを復号化する。さらに，受信者ＢはICカード50

0内の一方向性関数手段5008を用いて，公開情報である一方向性関数ｆから共通鍵ＫをK=f(m)により計算し，共通鍵Kを受信者側装置に出力する。

上述の様に，本実施例では，一方向性関数を組み合わせて，使用することにより，送信データｍ自身は外部へ出力しない。このように，ICカード（または，計算カード）など個人が携帯する周辺機器内部で，暗号化および復号化を行うことで，選択暗号文攻撃を許さない，すなわち，能動的攻撃に対しても安全な環境を作ることができる。

【０２５４】

また，メッセージそのものを本発明による公開鍵暗号方法を用いて送信する構成においては，本実施例のアプリケーションBプログラム2005が復号化したメッセージを所定のルールによって解釈し，意味のないメッセージが復号されたと判断した場合，そのメッセージを外部機器に出力することなく消去するなどして，能動的攻撃を許さない環境を作ることができる。

【０２５５】

上述のように，本実施例は一方向性関数を組み合わせて使用することにより，さらに，能動的攻撃に対しても安全な環境を作るものである。

【０２５６】

（実施例15）

本実施例は実施例１３の基本形である。

【０２５７】

実施例１３において，d=1とし，送信者は，送信データｍ（0<m<ｎ）に対して，前記暗号化方法にて暗号文C,Dを作成し，暗号文C,Dを受信者に送信する。

【０２５８】

受信者は，保持している上記秘密情報2007と，受信者側装置200内の復号化手段2004、べき乗算手段2002，剰余演算手段2003を用いて，

【０２５９】

【数１１２】

$$m^2 = CD^s \bmod n, \qquad \cdots (数112)$$

【０２６０】

にて，暗号文Ｃ，Ｄから送信データｍを復号化する。

【０２６１】

本実施例による方法では，前提を置くことなく，完全解読の困難性と素因数分解問題の困難性の等価性，および，部分解読の困難性とDiffie-Hellman決定問題の困難性の等価性を示すことができる。

【０２６２】

また，本実施例では，送信データmの範囲を実施例１３に比べて広く取れるため，実施例１３に比べて長いメッセージを送ることが可能である。

【０２６３】

（実施例16）

実施例7と同様に、実施例１３から実施例１５においても、

【０２６４】

【数１１３】

$$g^r \bmod n, \quad h^r \bmod n \qquad \cdots \text{(数113)}$$

【０２６５】

の計算は，送信データmに関係しないため，前処理が可能である。これにより，暗号化時間を大幅に短縮することが可能となる。

【０２６６】

なお、すでに述べたように、上記各実施例において、ｄ（ｄ≧１）の値をｎの素因数分解が困難である範囲において，大きく選ぶことで，ｎのビット数が一定の場合，ｐのビット数が小さくなるため，復号化処理を高速に行うことが出来る。このｄの値を、第3者側装置あるいは、受信者側装置にて管理すれば、計算機能力の発展、素因数分解に必要とされる計算時間と安全性との関係などによって、変えることが可能である。

【０２６７】

また、上記各実施例における送信データmには、通常の秘密に送信したいメッセージのほか、共通鍵暗号方法に用いる共通鍵、メッセージ認証に用いるメッセ

ージとメッセージ認証子を合わせたものが当てはまる。

【０２６８】

また，本実施例では，送信者と受信者が各々の装置を利用して暗号通信を行うという一般形で述べたが，具体的には様々なシステムに適用される。

【０２６９】

例えば，電子ショッピングシステムでは，送信者はユーザであり，送信者側装置はパソコンなどの計算機であり，受信者は小売店，受信者側装置はパソコンなどの計算機となる。このとき，ユーザの商品等の注文書は共通鍵暗号方法で暗号化されることが多く，その際は、暗号化鍵を本発明による鍵共有（鍵配送）方法により暗号化して小売店側装置に送信される。

【０２７０】

また，電子メールシステムでは，各々の装置はパソコンなどの計算機であり，送信者のメッセージは共通鍵暗号方法で暗号化されることが多い。その際も、暗号化鍵は、本発明による鍵共有（鍵配送）方法を用いて暗号化して受信者の計算機に送信される。

【０２７１】

その他にも，従来の公開鍵暗号が使われている様々なシステムに適用することが可能である。

【０２７２】

なお、本実施例における各計算は、CPUがメモリ内の各プログラムを実行することにより行われるものとして説明したが、プログラムではなく、いずれかがハードウェア化された演算装置であって、他の演算装置やCPUと、データのやりとりを行うものであってもよい。

【０２７３】

【発明の効果】

本発明によれば，安全で、高速処理が可能な、公開鍵暗号方法と、その応用装置、システムを実現することができる。

【図面の簡単な説明】

【図１】

本発明の各実施例のシステム構成を示す図である。

【図２】

本発明の実施例におけるICカードの内部構成を示す図である。

【図３】

本発明の実施例１の概要を示す図である。

【図４】

本発明の実施例３の概要を示す図である。

【図５】

本発明の実施例による方式と代表的な実用的公開鍵暗号方式との効率性（モジュラー積の個数）の比較を表す図である。

【図６】

本発明の実施例６の概要を示す図である。

【符号の説明】

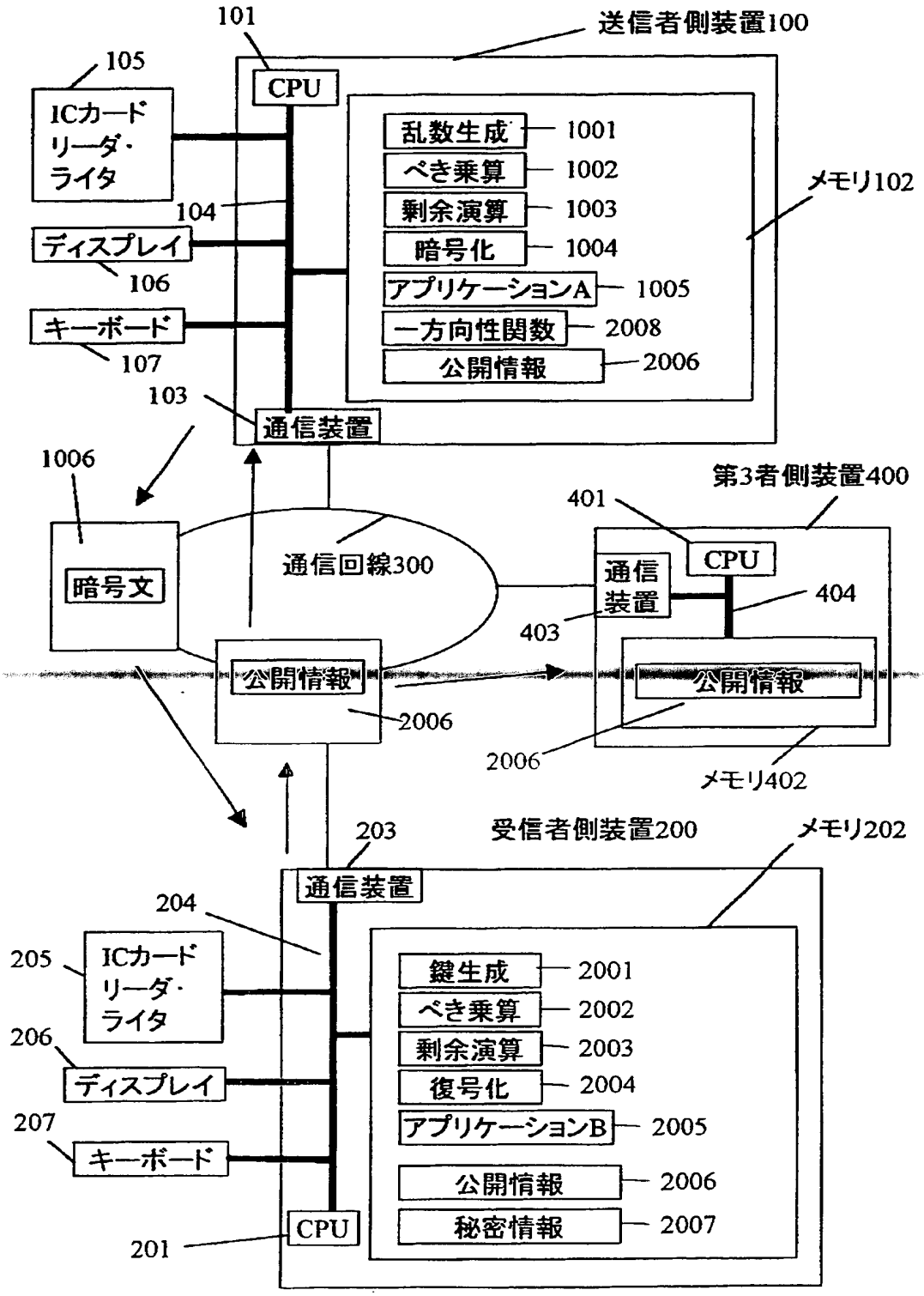
１００…送信者側装置，１０１…送信者側装置１００内のＣＰＵ，１０２…送信者側装置１００内のメモリ，１０３…送信者側装置１００内の通信装置，１００１…送信者側装置１００内の乱数生成手段，１００２…送信者側装置１００内のべき乗算手段，１００３…送信者側装置１００内の剰余演算手段，１００４…送信者側装置１００内の暗号化手段，２００…受信者側装置，２０１…受信者側装置１００内のＣＰＵ，２０２…受信者側装置２００内のメモリ，２０３…受信者側装置２００内の通信装置，２０４…受信者側装置２００内のＩＣカードリーダライタ，２００１…受信者側装置２００内の鍵生成手段，２００２…受信者側装置２００内のべき乗算手段，２００３…受信者側装置２００内の剰余演算手段，２００４…受信者側装置２００内の復号化手段，２００６…公開情報，２００７…秘密情報，５００…受信者のＩＣカード，５０１…ＩＣカード５００内のＣＰＵ，５０２…ＩＣカード５００内のメモリ，５０３…ＩＣカード５００内のＩ／Ｏ，５００１…ＩＣカード５００内の鍵生成手段，５００２…ＩＣカード５００内のべき乗算手段，５００３…ＩＣカード５００内の剰余演算手段，５００４

…ＩＣカード５００内の復号化手段，５００８…ＩＣカード５００内の一方向性関数手段。

【書類名】　図面

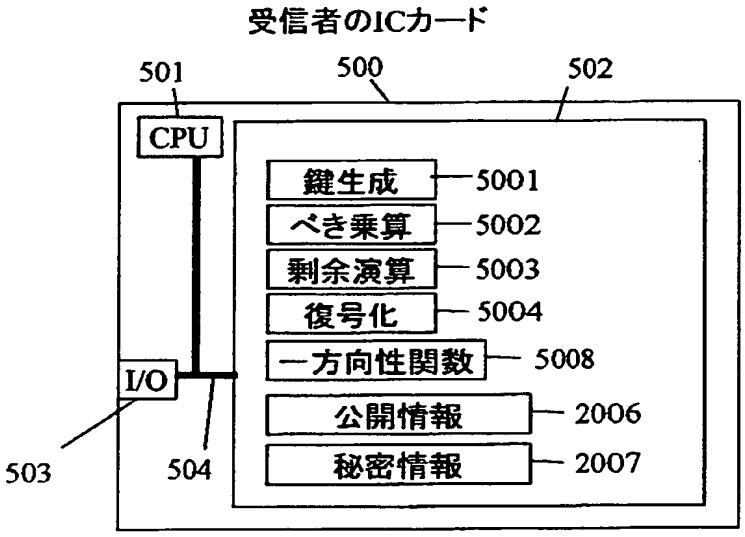
【図１】

図1


101
送信者側装置100
105
CPU
ICカード
リーダ・
ライタ
乱数生成
1001
べき乗算
1002
剰余演算
1003
暗号化
1004
アプリケーションA
1005
一方向性関数
2008
公開情報
2006
メモリ102
104
ディスプレイ
106
キーボード
107
103
通信装置
1006
暗号文
通信回線300
第3者側装置400
401
CPU
通信
装置
404
403
公開情報
公開情報
2006
2006
メモリ402
203
受信者側装置200
メモリ202
通信装置
204
205
ICカード
リーダ・
ライタ
206
ディスプレイ
207
キーボード
鍵生成
2001
べき乗算
2002
剰余演算
2003
復号化
2004
アプリケーションB
2005
公開情報
2006
秘密情報
2007
CPU
201

【図２】

図2


受信者のICカード
501
500
502
CPU
I/O
503
504
鍵生成
5001
べき乗算
5002
剰余演算
5003
復号化
5004
一方向性関数
5008
公開情報
2006
秘密情報
2007

【図３】

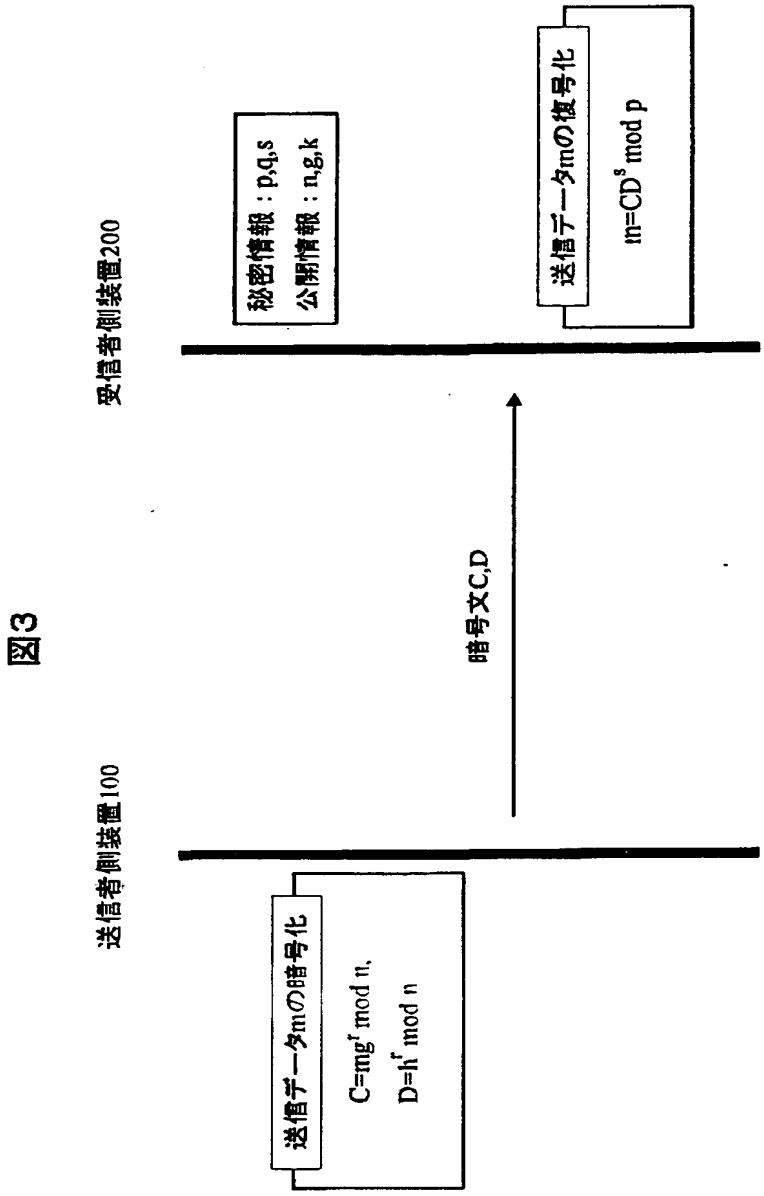
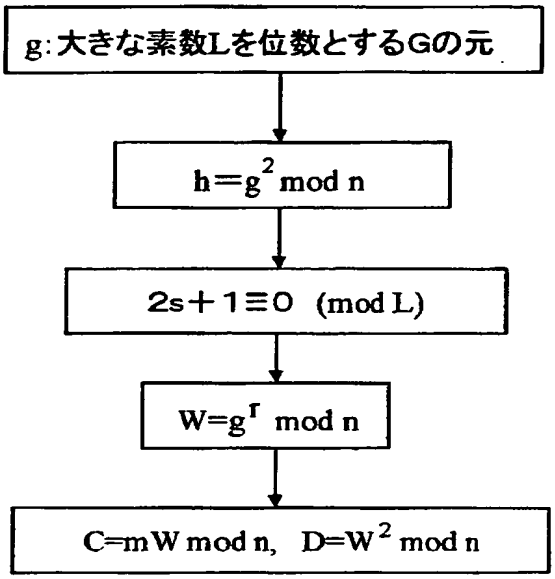

受信者側装置200
秘密情報：p,q,s
公開情報：n,g,k
送信データmの復号化
m=CD^s mod p
暗号文C,D
送信者側装置100
送信データmの暗号化
C=mg^r mod n,
D=h^r mod n

図3

【図４】

図4



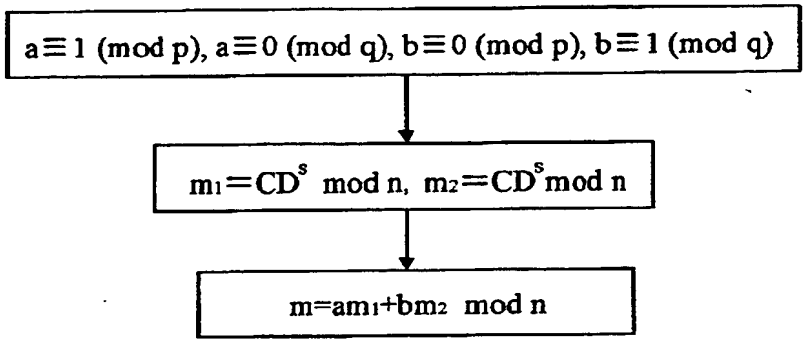
【図５】

図5

	暗号化	復号化
RSA	約 2～1500	約 400
ElGamal暗号	約 3000	約 1500
EPE	約 13	約 400
EPOC	約 230	約 230
本発明の方式	約 200	約 60

【図６】

図6


a≡1 (mod p), a≡0 (mod q), b≡0 (mod p), b≡1 (mod q)
m1=CD^s mod n, m2=CD^s mod n
m=am1+bm2 mod n

【書類名】　要約書

【要約】

【課題】

受信者の公開鍵を用いて，送信データを暗号化する公開鍵暗号による暗号通信方法であって，安全性の証明が可能であり，かつ，効率性の高い処理ができる公開鍵暗号方法および装置を提供する。

【解決手段】

受信者は，受信者側装置200を用いて，秘密鍵として（p,q,s）を作成し，公開鍵として（n,g,k）を作成する（但し，kはp,qのビット長）。

送信者は，送信者側装置100を用いて，乱数r（$0<r<2^{k-1}$）を選び，送信データm（$0<m<2^{k-1}$）について，$C=mg^r \bmod n$，$D=g^{2r} \bmod n$を計算して、暗号化する。

受信者は、受信者側装置200を用いて、暗号文C、Dについて$m=CD^s \bmod p$により，送信データmに復号化する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所